Appendix A High Level Requirements Traceability Matrix

Арреника	High Level Requirements Traceability Matrix			
No	Requirement The System Shall	Area	Sub-Area	Use Case
1	Allow an administrator to enroll new users for the mDL program	Core Functions	Administrative Functions	Enroll in the mDL Program
	, , , , , , , , , , , , , , , , , , ,			30.7
2	Allow an administrator to associate an existing traditional driver's license with a mDL	Core Functions	Administrative Functions	Enroll in the mDL Program
3	Allow an administrator to view existing mDL enrollments	Core Functions		Enroll in the mDL Program
	Provide the ability to determine if a prospective user is eligible for enrollment into the			2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
4	mDL program	Core Functions	Administrative Functions	Enroll in the mDL Program
5	Allow an administrator to cancel the mDL enrollment process	Core Functions		Enroll in the mDL Program
6	Capture requests for enrollment into the mDL program	Core Functions	User Functions	Enroll in the mDL Program
				· ·
7	Present disclaimers, terms and conditions for new enrollments in to the mDL program	Core Functions	User Functions	Enroll in the mDL Program
	Ensure that disclaimers, terms and conditions for new enrollments in to the mDL program			
8	have been accepted before enrolling the user	Core Functions	User Functions	Enroll in the mDL Program
	Create a record that the disclaimers, terms and conditions for new enrollments in to the			-
9	mDL program have been accepted	Core Functions	User Functions	Enroll in the mDL Program
10	Allow new users enroll in the mDL program	Core Functions	User Functions	Enroll in the mDL Program
	Provide the user with a single use secure credential to be used for initially authenticating			
11	the user's identity through their mobile device	Core Functions	User Functions	Enroll in the mDL Program
12	Deliver instructions for acquiring and configuring the mDL application to the user	Core Functions	User Functions	Enroll in the mDL Program
13	Capture requests for enrollment into the mDL program	Core Functions	User Functions	Enroll in the mDL Program
14	Allow the user to cancel the mDL enrollment process	Core Functions	User Functions	Enroll in the mDL Program
15	Notify a user that their mDL has been issued	Core Functions	User Functions	Procure a mDL
13	Notify a aser that their more has been issued	Core i unecions	OSCI T UNICUONS	Trocare a mb2
16	Provide a means for the user to install or enable mDL application on their mobile device	Core Functions	User Functions	Procure a mDL
10	Trovace a fricality for the agent to motality of chapter may appropriate from their mostile device	COTE T UNICEIONS	oser ranceions	Trocare a mou
17	Provide a means for the user to access the mDL application on their mobile device	Core Functions	User Functions	Procure a mDL
18	Authenticate a user's secure single use credential	Core Functions	User Functions	Procure a mDL
19	Allow initial login to the mDL application using a single use credential	Core Functions	User Functions	Procure a mDL
20	Ensure that a user creates new credentials after their first login to the mDL	Core Functions	User Functions	Procure a mDL
20	Ensure that a user creates new createnants after their instringin to the inst	Core runctions	OSCI T UNICUONS	Trocare a mbz
21	Enable display of mDL only after a user has logged in using their credentials	Core Functions	User Functions	Procure a mDL
22	Enable authentication of mDL only after a user has logged in using their credentials	Core Functions	User Functions	Procure a mDL
23	Associate privileges with a user mDL	Core Functions		Update privileges associated with a mDL
24	Allow administrators to add associated privileges to a user mDL	Core Functions		Update privileges associated with a mDL
	The second to add associated principles to a doct more	23.0.1 0.10010113		Transportation with a more
25	Allow administrators to remove associated privileges from a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL
23	Anow autimistrators to remove associated privileges from a user mot	Core Functions	Administrative runctions	Opuate privileges associated with a HIDL
26	Allow administrators to suspend privileges associated with a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL
20	Philose duffilliations to susperiorprivileges associated with a user Hibb	Core i unictions	Administrative runctions	opuate privileges associated with a HDL
27	Allow administrators to reinstate privileges associated with a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL
		123.0. 4.100013		1 - p p p

28	Notify a user that the privileges associated with their mDL have been updated	Core Functions	User Functions	Update privileges associated with a mDL
29	Update the privileges displayed on a mDL to reflect updates made by administrators	Core Functions	User Functions	Update privileges associated with a mDL
30	Update the privileges that can be presented with a mDL to reflect updates made by administrators	Core Functions	User Functions	Update privileges associated with a mDL
31	Prevent authentication of the mDL unless the user permits it	Core Functions	User Functions	Authenticate mDL
31	The value and the time and the deep permits to	Core i uneciono	Coci i dileciono	rational and a second a second and a second
32	Prevent access to the mDL unless the user authenticates using secure credentials	Core Functions	Technical	Authenticate mDL
33	Allow an authenticator to validate an mDL	Core Functions	Authentication Function	Authenticate mDL
34	Allow an authenticator to flag abuse of a mDL	Core Functions	Authentication Function	Authenticate mDL
35	Notify the administrator of mDLs that have been flagged for abuse	Core Functions	Administrative Functions	Authenticate mDL
36	Notify a user that their mDL has been flagged for abuse	Core Functions	User Functions	Authenticate mDL
37	Allow an administrator to invalidate a mDL that has been flagged	Core Functions	Administrative Functions	Authenticate mDL
38	Allow an administrator to reinstate a mDL that has been flagged	Core Functions	Administrative Functions	Authenticate mDL
39	Periodically synch and update the status of a mDL	Core Functions	Technical	Authenticate mDL
40	Present a timestamp on the mDL demonstrating the last update of the mDL	Core Functions	Technical	Authenticate mDL
41	Prevent access to view the privileges associated with the mDL unless the user permits it	Core Functions	User Functions	View privileges associated with a mDL
42	Display privileges associated with the users mDL	Core Functions	User Functions	View privileges associated with a mDL
43	Allow a user to select the subset of privileges to display	Core Functions	User Functions	View privileges associated with a mDL
44	Display personal information associated with the users mDL	Core Functions	User Functions	View mDL personal information
45	Allow a user to select the subset of personal information to display	Core Functions	User Functions	View mDL personal information
	Prevent access to view the personal information associated with the mDL unless the user			
46	permits it	Core Functions	User Functions	View mDL personal information
47	Notify the user that a request to update their mDL information has been captured	Core Functions	Administrative Functions	Update mDL Personal Information
48	Allow the administrator to review requests for mDL information updates	Core Functions	Administrative Functions	Update mDL Personal Information
49	Allow the administrator to approve or deny requests for mDL information updates	Core Functions	Administrative Functions	Update mDL Personal Information
50	Display updated information on a users mDL	Core Functions	User Functions	Update mDL Personal Information
30	Display apaated information on a asers the	Core runctions	OSCI I dilections	opaate mbe reisonal mormation
51	Provide administrators with the ability to dis-enroll existing users from the mDL program	Core Functions	Administrative Eurotions	Dis-enroll from the mDL Program
52	Provide users with the ability to dis-enroll from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
<u> </u>	Trovide users with the ability to dis emon from the mbe program	Core i unecions	OSCI I dilettoris	Dis cirroli from the finde frogram
53	Ensure that users are authenticated when dis-enrolling from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
54	Ensure that users confirm their intent to dis-enroll from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
54	Ensure that users commit their intent to dis-enroll from the first program	COTE I UTICUOTIS	O3ELL ULICUOUS	DIS CHIOH HOHI the HIDL Flogram
55	Provide a confirmation once a user has been dis-enrolled from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
	Disable all mDL authentication and display functions on the user's devices once a user is			
56	dis-enrolled	Core Functions	User Functions	Dis-enroll from the mDL Program
E 7	Burgo any mBL related data that is stored remetely once a user is dis enrolled	Extended Eurotic	nd Tochnical	Dis appell from the mDI Program
57	Purge any mDL related data that is stored remotely once a user is dis-enrolled	Extended Function	ng recrimical	Dis-enroll from the mDL Program

58	Display a 2-d barcode that encodes the user's driver's license information	Extended Functions	Stakeholder Functions	Scan mDL barcode
59	The displayed 2-d barcode must be compliant with the existing standard used for physical driver's licenses	Extended Functions	Technical	Scan mDL barcode
	Ensure that displayed 2-d barcode can be scanned with a barcode scanner (maximize			
60	brightness and contrast of the screen)	Extended Functions	Technical	Scan mDL barcode
61	Display the driver's license information of the user's mDL to an authenticator	Extended Functions	Authentication Function	Authenticate mDL manually
62	Display the user's driver's license picture to an authenticator	Extended Functions	Authortication Eurotion	Authenticate mDL manually
02	Display the user's driver's license picture to an authenticator  Display security features (like a randomized token) that can be used by an authenticator to		Authentication Function	Authenticate IIIDE Manually
63	manually validate a mDL by calling into a hotline or dispatch	Extended Functions	Technical	Authenticate mDL manually
- 55	mandally randate a more by caning mee a notine of angularing	Externaca ranotions	rediffical	Authenticate mDL digitally, in a disconnected
64	Provide the ability to authenticate with another digital device	Extended Functions	Technical	state
				Authenticate mDL digitally, in a disconnected
65	Provide the ability to communicate with another digital device	Extended Functions	Technical	state
				Authenticate mDL digitally, in a disconnected
66	Request permission from the user before initiating communication with another device	Extended Functions	Technical	state
	Automatically revoke further access to communicate with a user's mDL after the			Authenticate mDL digitally, in a disconnected
67	interaction with the authenticator is complete	Extended Functions	Technical	state
68	Allow the mDL to remotely authenticate	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
- 55		Externaca ranscrons	rediffical	3.3.77
69	Provide secure remote attestation of user identity to digital authentication devices	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
70	Allow the authenticator to remotely retrieve privileges associated with the mDL	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
71	Allow the authenticator to remotely retrieve information associated with the mDL	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
71	Allow a stakeholder or authenticator to digitally retrieve privileges associated with the	Exteriored i directions	recinical	nationicate instantant, in a connected state
72	mDL	Extended Functions	Technical	Electronically access mDL information
	Allow a stakeholder or authenticator to digitally retrieve information associated with the			,
73	mDL	Extended Functions	Technical	Electronically access mDL information
	Request permission from the user to transmit privileges associated with the mDL to			
74	another device	Extended Functions	Technical	Electronically access mDL information
75	Request permission from the user to transmit information associated with the mDL to	5 . I I 5 .:		5
75	another device	Extended Functions	Technical	Electronically access mDL information
	Automatically revoke further access to communicate with a user's mDL after transmission			
76	of information associated with the mDL to another device is complete	Extended Functions	Technical	Electronically access mDL information
				, , , , , , , , , , , , , , , , , , , ,
	Automatically revoke further access to communicate with a user's mDL after transmission			
77	of privileges associated with the mDL to another device is complete	Extended Functions	Technical	Electronically access mDL information
	Notify a user that a request has been made to digitally transmit privileges associated with			
78	the user's mDL	Extended Functions	Use Functions	Electronically access mDL information
	In order to facilitate interoperability across jurisdictions, the mDL, the mDL reader, and its			
	related infrastructure will comply where possible with draft ISO18013 technical requirements. Any variances where the solution does not follow the draft ISO18013			
	technical requirements will be documented by the vendor and subject to Department			
79	approval.	Extended Functions	Technical	Electronically access mDL information
	Notify a user that a request has been made to digitally transmit information associated			,
80	with the user's mDL	Extended Functions	User Functions	Electronically access mDL information
-				

81	Store a record certifying that a mDL has been digitally validated	Extended Functions	Technical	Record mDL validation
31	Return a key to the authenticator which corresponds to the record certifying that a mDL	zateriaca i unctions	. common	THE PURCHASION
82	has been digitally validated	Extended Functions	Technical	Record mDL validation
	Retrieve a record corresponding to an authentication key certifying that a mDL has been	Externaca i arrotrorio	. commou	The state of the s
83	digitally validated	Extended Functions	Technical	Record mDL validation
	Provide access to appropriate functions for mDL users, administrators, stakeholders and			
84	authenticators	Non-Functional	Accessibility	N/A
	Provide a user interface that is navigable by and accessible to all users of supported		,	
85	mobile platforms (including those with disabilities)	Non-Functional	Accessibility	N/A
	Integrate with the lowa DoT's existing licensing and administrative systems, preserving			
86	their roles as systems of record	Non-Functional	Architecture/Integration	N/A
	Be developed using an advanced approach to interoperability using web services and			
	Service Oriented Architecture (SOA) allowing for all major administrative functions to be			
87	completed through Web Service APIs	Non-Functional	Architecture/Integration	N/A
	Consist of a number of components and services that are compliant with industry			
	standards for service-oriented architecture and Web Services (W3C, OASIS, etc.) to			
88	facilitate reuse, adaptability and interoperability	Non-Functional	Architecture/Integration	N/A
		ns to be Non-Functional Architecture/Integration N/A  Non-Functional Architecture/Integration N/A  Non-Functional Architecture/Integration N/A  e mDL Non-Functional Architecture/Integration N/A  audit trail and Non-Functional Audit N/A  lata, Non-Functional Audit N/A		
89	Ensure secured access to services based on defined security rules	Non-Functional	Architecture/Integration	N/A
	Interface with Iowa DoT's systems of record through Web Service APIs and enable mDL			
90	program functions to be incorporated into the workflows of those systems	Non-Functional	Architecture/Integration	N/A
	Provide audit-tracking reports for user access and usage logs including a detailed audit trail			
	for a select set of system transactions, activities and actions, including date, time and			
91	author	Non-Functional	Audit	N/A
	Have the ability to provide an audit trail for changes, additions and deletions to data,			
92	including operational and security data	Non-Functional	Audit	N/A
93	Be available for use 999% of the time (no more than 88 hours of downtime per year)			
94	Operate 24 hours per day, 7 days per week, and 52 weeks per year	Non-Functional	Availability	N/A
05	Have the ability to support transparent failover using high-availability processor	Non-Franchismal	A 11 - 1- 1114	21/2
95	architectural options	Non-Functional	Availability	N/A
06	Be able to continue to operate despite failure or availability of individual technology	Non Functional	Availability	NI/A
96	components such as a server platform or network connection  Be able to handle the initial launch storage and processing loads while growing to serve	Non-Functional	Availability	N/A
97	growth of the user base	Non-Functional	Capacity	N/A
31	Maintain compatibility with major supported mobile platforms (Android, iOS) and a	14011 I unctional	Capacity	1975
98	defined range of OS versions	Non-Functional	Device Compatibility	N/A
50	Be compatible with leading devices (Apple iPhone, Samsung Galaxy S series, etc.) which		207100 COMPARISHING	.,,,
99	support the hardware requirements of the mDL application	Non-Functional	Device Compatibility	N/A
	Be compatible with a well defined range of mobile screen sizes, resolutions and form			
100	factors	Non-Functional	Device Compatibility	N/A
	Be implemented such that the mDL application is not degraded as a result of minor OS		, ,	
	version updates (e.g. use stable APIs, avoid deprecated features, avoid niche or dated 3rd			
101	party libraries etc.)	Non-Functional	Device Compatibility	N/A
	Make use of platform standards and features developed by mobile platform makers (e.g.			
102	digital wallet APIs, biometric features, push notifications etc.)	Non-Functional	Device Compatibility	N/A
	Be implemented to efficiently use the mobile battery and avoid unnecessary drain on the			
103	mobile devices processing resources	Non-Functional	Device Compatibility	N/A

10.5   Secondecide set.		Ensure the mDL application functions in a various states of connectivity (cellular data, wifi,			
105 Preserve data integrity, fall safe and trap bad data and faults 106 Be designed for ease of ministeriance and readily allow fature functional enhancements 107 Be adequately flexible to keep up with ever changing technology and regulations 108 application responsiveness at all times 108 application responsiveness at all times 109 future 110 Provide a high levels of performance, with acceptable response and processing times and 1110 Provide responsiveness at all times 1111 African and the factor of the state of the performance of the factor	104		Nan Frankisası	Davies Commetibility	N1/A
105 Be designed for ease of maintenance and readily allow future functional enhancements 107 Be adequately fleuble to keep up with ever changing technology and regulations 108 application responses at all times 109 focuse is high levels of performance, with acceptable response and processing times and 109 future 110 focuse response times of less than 5 seconds at all times 110 focuse response times of less than 5 seconds at all times 111 flave seamiless State recovery and backup processes 112 Adhere to all applicable legal, statutory, and regulatory requirements 113 flave a low defect/fuller rate 114 change in user population, transaction volume, throughput and geographical distribution 115 fliering capabilities scalable to accommodate changes in system scale including 116 changes in user population, transaction volume, throughput and geographical distribution 117 own specific needs within a profile aligned to the analytic role of each user 118 accidental cause 119 regulations and must be easy to build and modify by the administrative users 119 regulations and industry best practices 110 able to view subsets of mDir related data based on user security profities and must be easy to underly the scandination of the formation of the provised basis to substitution of the formation of the provised basis to substitute of the formation		·			
107 Be adequately Resible to keep up with ever changing technology and regulations Provide a high levels of performance, with acceptable response and processing times and pagilication responseries at all times 108 Be built to scale such that large increases users and usage can be accommodated in the future 110 Provide response times of less than 5 seconds at all times 110 Provide response times of less than 5 seconds at all times 111 Auto-seamless disaster recovery and bockup processes 112 Adhere to all applicable legal, statutory, and regulatory requirements 113 Allaw a low defect/failure rate 114 Auto-seamless disaster recovery and bockup processes 115 Allaw a low defect/failure rate 116 Provide reporting capabilities scalable to accommodate changes in system scale including 117 Auto-scale in user population, transaction volume, throughput and geographical distribution 118 Auto-scale in user population, transaction volume, throughput and geographical distribution 119 Provide the ability to build reports and save report templates These reports will have 110 Provide the ability to build reports and save report templates These reports will have 111 Auto-scale in user population, transaction volume, throughput and geographical distribution 116 Provide business intelligence tools to allow for searching, reporting, and reviewing data for own specific needs within a profile aligned to the analytic role of each user 119 Auto-scale in the security infrastruture and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to name and the security protection of programs and data from intentional unauthorized access attempts as well as security breaches due to name and the scale of the security and the scale of the security protection of programs and data from intentional unauthorized access attempts using a paporporiate understance and the scale of the sc	105	Preserve data integrity, rail sale and trap bad data and raults	Non-Functional	integrity	N/A
Provide a high levels of performance, with acceptable response and processing times and application responsewess at all times  109 Rebuilt to scale such that large increases users and usage can be accommodated in the future  110 Provide response times of less than 5 seconds at all times  111 After seamles disaster recovery and backup processes  112 Adhiere to all applicable legal, statutory, and regulatory requirements  113 Have sealmes disaster recovery and backup processes  114 Adhiere a to all applicable legal, statutory, and regulatory requirements  115 Adhiere to all applicable legal, statutory, and regulatory requirements  116 Provide reporting capabilities scalable to accommodate changes in system scale including changes in user population, transaction volume, throughput and geographical distribution  115 Provide the ability to build reports and save report templates These reports will have liftering capabilities and must be kasy to build and modify by the administrative users  116 management purposes  Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user  118 accidental causes  118 accidental causes  119 regulations and industry best practices  120 Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of multi-indicate abused as well as security phreaches due to allow for security principals and properties mechanism (e.g., locks the accountry finde abused on user security principals  121 that conditions and industry best practices  122 and provide the ability to identify certain information as confidential (e.g. Pii) and only make that accessibly by appropriately authorized users and authorities will be allowed to security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  122 a configurable display algorithm)  Provide the ability to identif	106	Be designed for ease of maintenance and readily allow future functional enhancements	Non-Functional	Maintainability	N/A
Provide a high levels of performance, with acceptable response and processing times and application responsewess at all times  109 Rebuilt to scale such that large increases users and usage can be accommodated in the future  110 Provide response times of less than 5 seconds at all times  111 After seamles disaster recovery and backup processes  112 Adhiere to all applicable legal, statutory, and regulatory requirements  113 Have sealmes disaster recovery and backup processes  114 Adhiere a to all applicable legal, statutory, and regulatory requirements  115 Adhiere to all applicable legal, statutory, and regulatory requirements  116 Provide reporting capabilities scalable to accommodate changes in system scale including changes in user population, transaction volume, throughput and geographical distribution  115 Provide the ability to build reports and save report templates These reports will have liftering capabilities and must be kasy to build and modify by the administrative users  116 management purposes  Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user  118 accidental causes  118 accidental causes  119 regulations and industry best practices  120 Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of multi-indicate abused as well as security phreaches due to allow for security principals and properties mechanism (e.g., locks the accountry finde abused on user security principals  121 that conditions and industry best practices  122 and provide the ability to identify certain information as confidential (e.g. Pii) and only make that accessibly by appropriately authorized users and authorities will be allowed to security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  122 a configurable display algorithm)  Provide the ability to identif					
108   application responsiveness at all times   Non-Functional   Performance   N/A	107		Non-Functional	Maintainability	N/A
Se built to scale such that large increases users and usage can be accommodated in the future   Non-Functional   Performance   N/A					
100	108		Non-Functional	Performance	N/A
110   Provide response times of less than 5 seconds at all times   Non-Functional   Recovery   N/A					
111 Have seamless disaster recovery and backup processes 112 Adhere to all applicable legal, statutory, and regulatory requirements 113 Adhere to all applicable legal, statutory, and regulatory requirements 114 Anve a low defect/failure rate 115 Provide reporting capabilities scalable to accommodate changes in system scale including changes in user population, transaction volume, throughput and geographical distribution 116 Provide the ability to build reports and save report templates These reports will have filtering capabilities and must be easy to build and modify by the administrative users 116 Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes 116 Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes 117 Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user 117 Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user 118 accordant causes 119 Reporting N/A 110 Reporting N/A 119 Reporting N/A 110 Reporting N/A 110 Reporting N/A 1110 Reporting N/A 1111 Reporting N/A 1112 Reporting N/A 1113 Reporting N/A 1114 Reporting N/A 1115 Reporting N/A 1116 Reporting N/A 1116 Reporting N/A 1116 Reporting N/A 1116 Reporting N/A 1117 Reporting N/A 1116 Reporting N/A 1117 Reporting N/A 1117 Reporting N/A 1118 Reporting N/A 1118 Reporting N/A 1118 Reporting N/A 1119 Reporting N/A 1119 Reporting N/A 1110 Reporting N/A 1110 Reporting N/A 1110 Reporting N/A 1110 Reporting N/A 1111 Reporting N/					
112 Adhrer to all applicable legal, statutory, and regulatory requirements  113 Have a low defect/failure rate  Non-Functional  Provide reporting capabilities scalable to accommodate changes in system scale including changes in user population, transaction volume, throughout and geographical distribution  Provide the ability to build reports and save report templates These reports will have filtering capabilities and must be easy to build and modify by the administrative users  Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes  Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user  Be implemented with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to accidental cause.  In gregulations and industry best practices  Allow for controlled access to participant records. Administrators and authorities will be abile to view subsets of mDL related data based on user security privileges  Allow for controlled access to participant records. Administrators and authorities will be abile to view subsets of mDL related data based on user security privileges  Allow for controlled access to participant records. Administrators and authorities will be abile to view subsets of mDL related data based on user security privileges  Allow for controlled access to participant records. Administrators and authorities will be abile to view subsets of mDL related data based on user security privileges  Allow for controlled access to participant records. Administrators and authorities will be abile to view subsets of mDL related data based on user security privileges  Ann-Functional  Protect against possibly malicious user authentication and information  Ann-Functional  Security  N/A  Protect against possibly malicious user authentication of information  a configura		·			1
113   Nave a low defect/failure rate   Non-Functional   Reliability   N/A				,	,
Provide reporting capabilities scalable to accommodate changes in system scale including changes in user population, transaction volume, throughput and geographical distribution Non-Functional Reporting N/A  Provide the ability to build reports and save report templates These reports will have filtering capabilities and must be easy to build and modify by the administrative users Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes  Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user own specific needs within a profile aligned to the analytic role of each user own specific needs within a profile aligned to the analytic role of each user own specific needs within a profile aligned to the analytic role of each user own specific needs within a profile aligned to the analytic role of each user own specific needs within a profile aligned to the analytic role of each user own specific needs within a profile aligned to the analytic role of each user own specific needs with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security prolicy and regulations and industry best practices of the profile aligned to the analytic role of each user own specific needs with a security prolicy and regulations and industry best practices of the profile aligned to					,
that changes in user population, transaction volume, throughput and geographical distribution  Provide the ability to build reports and save report templates These reports will have filtering capabilities and must be easy to build and modify by the administrative users  Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes  Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user  Be implemented with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to accidental causes  Interest and industry best practices  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security prolitices.  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security prolitices.  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security prolitices.  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security prolitices.  Allow for controlled access to participant records, administrator, on the provide the participant records. Administrator on the formation and the provide account/node of a configurable time period, or delays the next login prompt according to a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. Pil) and only make that accessible by appropriately authorized users  When storing private information on any device intended to be portable/removable (e.g. smartpho	113	Have a low defect/failure rate	Non-Functional	Reliability	N/A
115   filtering capabilities and must be easy to build and modify by the administrative users   Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes   N/A	114		Non-Functional	Reporting	N/A
Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes  Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user  Be implemented with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to accidental causes  Inspection of the controlled access attempts as well as security breaches due to accidental causes  Inspection of the controlled access attempts as well as security provided to accidental causes  Non-Functional  Security  N/A  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Non-Functional  Security  N/A  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable dime period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. Pil) and only make that accessible by appropriately authorized users  Non-Functional  Security  N/A  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 30ES, AES or their successors  Provide the capability to integrate with existing authentication and authorization  Non-Functional  Non-Functional  Security  N/A		Provide the ability to build reports and save report templates These reports will have			
Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user  Be implemented with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to 118 accidental causes  Implement security controls in accordance with all Federal and State security policy and regulations and industry best practices  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Security  N/A  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until relased by an administrator, locks the account/node or a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards assurance and authorization mechanisms used by the lowa DoT  Non-Functional	115	filtering capabilities and must be easy to build and modify by the administrative users	Non-Functional	Reporting	N/A
Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user  Be implemented with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to accidental causes  Inplement security controls in accordance with all Federal and State security policy and regulations and industry best practices  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Non-Functional  Security  N/A  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node of ra configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable format using 3DFS, AES or their successors  Non-Functional  Security  N/A  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable format using 3DFS, AES or their successors  Provide the capability to integrate with existing authentication and authorization  Non-Functional  Security  N/A		Provide business intelligence tools to allow for searching, reporting, and reviewing data for			
117 own specific needs within a profile aligned to the analytic role of each user  128 Be implemented with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to accidental causes  118 accidental causes  119 Implement security controls in accordance with all Federal and State security policy and regulations and industry best practices  120 Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  120 Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  121 Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node or a configurable time period, or delays the next login prompt according to a configurable time period, or delays the next login prompt according to a configurable time period, or delays the next login prompt according to Provide the ability to identify certain information as confidential (e.g. Pil) and only make that accessible by appropriately authorized users  122 Avenuable of the ability to identify certain information as confidential (e.g. Pil) and only make that accessible by appropriately authorized users  123 When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  124 Security N/A  125 Men accessible to the portable with existing authentication and authorization  126 Men accessible to the portable with existing authentication and authorization  127 Mon-Functional  128 Non-Functional  129 Non-Functional  120 Non-Functional  120 Non-Functional  121 Non-Functional  122 Non-Functional  123 Non-Functional  124 Security N/A  125 Non-Func	116	management purposes	Non-Functional	Reporting	N/A
data from intentional unauthorized access attempts as well as security breaches due to accidental causes  Implement security controls in accordance with all Federal and State security policy and regulations and industry best practices  Non-Functional Security  N/A  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional Security  N/A  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node on a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  Security  N/A  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional  Security  N/A  Provide the capability to integrate with existing authentication and authorization  mechanisms used by the lowa DOT  Non-Functional  Security  N/A	117	own specific needs within a profile aligned to the analytic role of each user	Non-Functional	Reporting	N/A
Implement security controls in accordance with all Federal and State security policy and regulations and industry best practices  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Non-Functional  Non-Functional  Security  N/A  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node or a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  Non-Functional  Non-Functional  Security  N/A  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional  Non-Functional  Security  N/A  Non-Functional  Security  N/A  Non-Functional  Security  N/A					
Implement security controls in accordance with all Federal and State security policy and regulations and industry best practices  Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  Security  N/A  Non-Functional  Security  N/A  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional  Provide the capability to integrate with existing authentication and authorization  mechanisms used by the lowa DOT  Non-Functional  Security  N/A					
Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Non-Functional  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  Security  N/A  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional  Security  N/A  Non-Functional  Security  N/A  Non-Functional  Security  N/A  Non-Functional  Security  N/A	118		Non-Functional	Security	N/A
Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Provide the capability to integrate with existing authentication and authorization mechanisms used by the lowa DoT  Non-Functional  Security  N/A  Non-Functional  Security  N/A					
able to view subsets of mDL related data based on user security privileges  Non-Functional  Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Non-Functional  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Provide the capability to integrate with existing authentication and authorization mechanisms used by the lowa DoT  Non-Functional  Security  N/A	119	regulations and industry best practices	Non-Functional	Security	N/A
Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional  Provide the capability to integrate with existing authentication and authorization mechanisms used by the lowa DoT  Non-Functional  Security  N/A	120		Non-Functional	Security	N/A
that could result from the loss, misuse, disclosure, or modification of information  Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional  Non-Functional  Security  N/A  Non-Functional  Security  N/A  Non-Functional  Security  N/A  Non-Functional  Security  N/A	120	able to view subsets of hibe related data based on user security privileges	Non i unctional	Security	IV/A
mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm)  Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  Non-Functional  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional  Non-Functional  Security  N/A  Provide the capability to integrate with existing authentication and authorization mechanisms used by the lowa DoT  Non-Functional  Security  N/A	121	,	Non-Functional	Security	N/A
Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional Security  N/A  Provide the capability to integrate with existing authentication and authorization mechanisms used by the lowa DoT  Non-Functional Security  N/A		mechanism (e.g. locks the account/node until released by an administrator, locks the			
that accessible by appropriately authorized users  When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Non-Functional Security  N/A  Provide the capability to integrate with existing authentication and authorization mechanisms used by the lowa DoT  Non-Functional Security  N/A	122	, <u> </u>	Non-Functional	Security	N/A
When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Provide the capability to integrate with existing authentication and authorization mechanisms used by the Iowa DoT  Non-Functional  Security  N/A					
smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors  Provide the capability to integrate with existing authentication and authorization mechanisms used by the Iowa DoT  Non-Functional  Security  N/A	123	that accessible by appropriately authorized users	Non-Functional	Security	N/A
Provide the capability to integrate with existing authentication and authorization  125 mechanisms used by the Iowa DoT Non-Functional Security N/A					
125 mechanisms used by the Iowa DoT Non-Functional Security N/A	124	based encrypted format using 3DES, AES or their successors	Non-Functional	Security	N/A
		Provide the capability to integrate with existing authentication and authorization			
Provide the capability to monitor events on the system, detect attacks, and provide	125	mechanisms used by the Iowa DoT	Non-Functional	Security	N/A
		Provide the capability to monitor events on the system, detect attacks, and provide			
126 identification of unauthorized use of the system Non-Functional Security N/A	126	identification of unauthorized use of the system	Non-Functional	Security	N/A

	Implement advanced security through biometric functions taking advantage of functions			
127	built into leading mobile phone platforms	Non-Functional	Security	N/A
128	Prevent unauthenticated access to the mDL application	Non-Functional	Security	N/A
	Bind biometric authentication methods to an instance of the mDL application to prevent			
129	impersonation of a user through the use of the mDL application	Non-Functional	Security	N/A
130	Communicate with other devices or networks only through encrypted connections	Non-Functional	Security	N/A
	Provide user interfaces that are easy and efficient to use and well as conform to look and			
131	feel standards	Non-Functional	Usability	N/A
	Support user-friendly navigation and interaction features that are easy to learn by a new			
132	end-user	Non-Functional	Usability	N/A

Comments

1
J

_
J

=